ServerView Operations Manager 連携のための基礎知識

2014 年 1 月
富士通株式会社

改版日	改版内容
2009.12.	新規作成
2014.1	JP1、千手との連携［新規]、他社運用管理ソフトウェア一覧の更新

はじめに

システムの安定稼動には、構成するサーバ、ネットワーク機器などが正常に動作しているか、期待通りに動作しているかをリアルタイム、かつ継続的に管理・監視する必要があります。

これを実現するためのソフトウェアが、一般的に「システム運用管理ソフトウェア」と呼ばれる製品（群）であり、多くのベンダーが、様々な製品を開発・展開しています。

FUJITSU Software ServerView® Suite は、「Deploy · Control · Dynamize · Maintain · Integrate」のサーバの運用サイクルを支援する製品群です。その中で、ServerView Operations Manager は、主に「サーバが正常に動作しているか」を管理·監視するサーバ運用監視ソフトであり、全ての FUJITSU Server PRIMERGY に、標準添付（無償）される形で、ユーザーに提供されます。

本資料の目的

本資料は、ServerView Operations Manager と共に他のシステム運用管理ソフトウェアの導入をご検討されている方、または、既にシステム運用管理ソフトウェアが導入されている環境に ServerView Operations Manager の導入をご検討されている方に、ServerView Operations Manager とシステム運用管理ソフトウェアとの連携を考える上で必要な基礎知識について、ご説明することを目的としています。

本資料を利用するにあたっての前提知識

本資料を利用するにあたって、以下の技術情報についての知識が必要となります。

- PC サーバに関する一般的な知識。
- Windows、Linux 等の OS に関する一般的な知識。
- ネットワークに関する一般的な知識。

本資料を活用するにあたっての留意事項

本資料は、2014 年 1 月現在の情報を元に作成しています。最新の ServerView Operations Manager の情報については、ServerView® Suite のマニュアルの「ServerView Operations Manager 取扱説明書」を、ServerView Agents の情報については、「ServerView Agents ユーザーガイド」を、システム運用管理ソフトウェアについて、各製品のマニュアルを参照してください。

本資料では、ServerView Operations Manager と ServerView Agents で構成される監視システムを ServerView と呼称します。

目次

1. 基礎知識

ServerView® Suite に限らず、システム運用管理ソフトウェアは、「SNMP」と「MIB」という２つの標準規格に大きく依存しています。

ここでは、本資料や ServerView® Suite のマニュアルなどを読む上で、最低限知っておきたい「SNMP」と「MIB」の基本事項について解説します。

1.1 システム運用管理ソフトウェアにおける SNMP と MIB の役割

システム運用管理ソフトウェアは、SNMP と MIB という 2 種類の標準規格を利用して、基本動作を実現しています。ServerView® Suite も、この標準規格を利用しています。

図 1-1 は、システム運用管理ソフトウェアにおいて、SNMP と MIB がどのような役割を果たしているかを、簡単に示した図です。

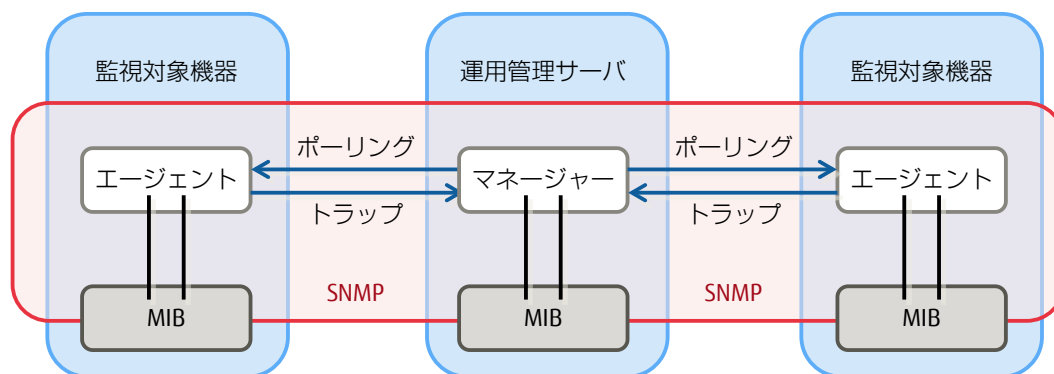



図 1-1 システム運用管理ソフトウェアにおける SNMP と MIB の役割

- **SNMP （Simple Network Management Protocol）**

  ネットワークシステムを監視・管理するためのプロトコルで、システム運用管理ソフトウェアに広く利用されています。システム運用管理ソフトウェアは、運用管理サーバ上にある「マネージャー」と監視対象機器に常駐する「エージェント」で構成され、その「マネージャー」と「エージェント」の通信に利用されているのが SNMP です。

  なお、「マネージャー」と「エージェント」に該当する機能の名称は、システム運用管理ソフトウェアによって異なる場合があります（ServerView® Suite では、「SNMP マネージャー」の機能に、「ServerView Operations Manager」という名称を用いています）。

- **MIB （Management Information Base）**

  システム運用管理ソフトウェアの「エージェント」が、監視対象機器の情報を取得するためには、MIB と呼ばれる「管理情報ベース」を参照します。「マネージャー」は、「エージェント」が取得した MIB の内容から、監視対象機器のどの部分で異常が発生したのか、どの部分が指定したしきい値に達したのかを判断します。「エージェント」が取得した MIB 情報を「マネージャー」が判断するために、**「エージェント」と「マネージャー」は共通の MIB を保有する必要があります。**

- ポーリング

  監視対象機器の「エージェント」に対して「マネージャー」が一台ずつ、定期的に検査や送信要求の確認のために問い合わせを行います。問い合わせ間隔が短いほどリアルタイム性は向上しますが、通信トラフィックやサーバ負荷が上がるため、設計時にはバランスが求められます。

- トラップ（**SNMP** トラップ）

  監視対象機器に常駐する「エージェント」は、指定したイベントが発生した場合や指定したしきい値に達した場合などに、「マネージャー」に状況通知レポートを送信します。この通知レポートを「SNMP トラップ」と呼びます。

SNMP、MIB のバージョンや MIB の構造などの情報については、添付資料にまとめてありますので、必要に応じて、参照してください。

2. ServerView Operations Manager とシステム運用管理ソフトウェアとの連携

本章では、ServerView Operations Manager を他のシステム運用管理ソフトウェアと連携する仕組みについて、「SNMP トラップ連携による方法」と、「イベントログを経由する方法」の２つをご紹介します。

2.1 SNMP トラップ連携による方法

SNMP トラップ連携により、ServerView Operations Manager とシステム運用管理ソフトウェアとの連携を実現する方法です。現在 ServerView Operations Manager と SNMP トラップ連携が可能なシステム運用管理ソフトウェアは、2.3.3 章をご参照ください。

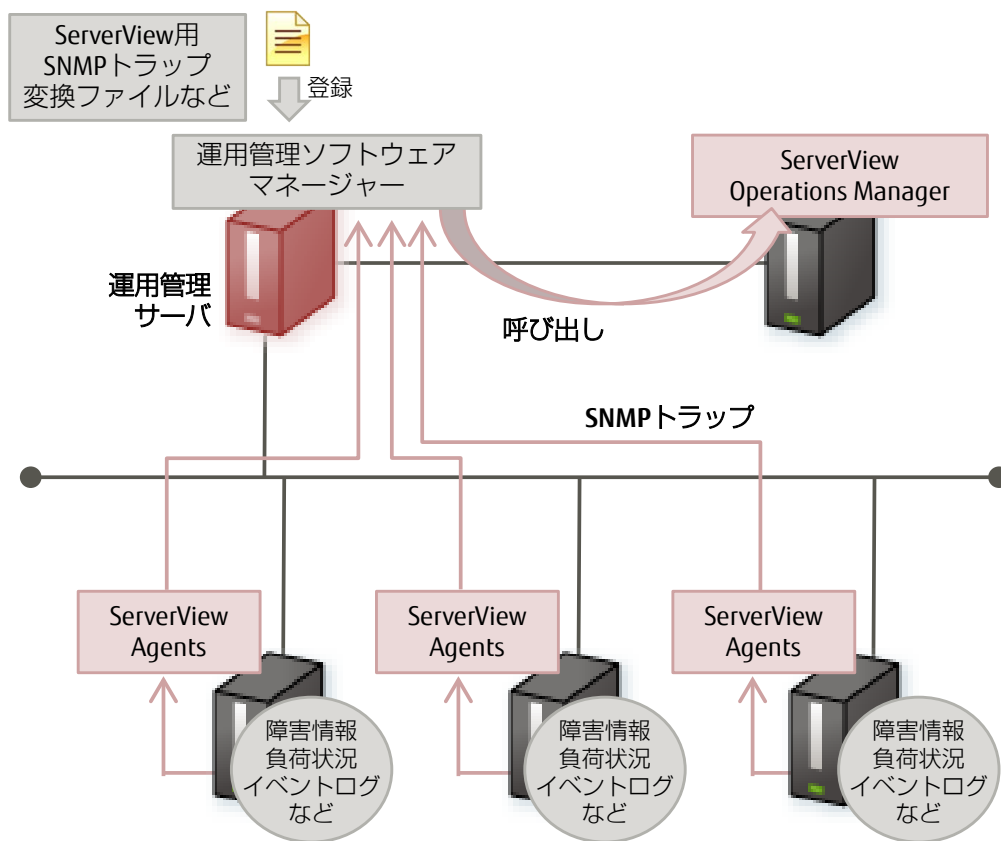



図 2-1 SNMP トラップ連携による ServerView とシステム運用管理ソフトウェアの連携イメージ

SNMP トラップ連携による ServerView Operations Manger とシステム運用管理ソフトウェアの連携は、ServerView Agents からの SNMP トラップを運用管理サーバが受信し、システム運用管理ソフトウェアの監視画面にログやアラート、メッセージの表示を行うなど高度な連携が行えます。

SNMP トラップ連携を行うには、事前にいくつかの設定を行う必要があります。

● SNMP トラップ連携に必要な操作

システム運用管理ソフトウェアによって操作順序の違いや、追加で必要な操作、不要な操作があります。詳細は「ServerView Operations Manager 取扱説明書」を参照してください。

- **監視対象サーバ上で SNMP サービスのトラップ先を変更**

  監視対象サーバの OS の SNMP サービスで、トラップ先を運用管理サーバに設定します。この設定が行われていない場合、システム運用管理ソフトウェアのマネージャーがトラップ通知を受信できないため、SNMP トラップ連携は動作しません。

- **メッセージテキスト変換ファイルの登録**

  ServerView Agents からの SNMP トラップを、システム運用管理ソフトウェアのマネージャー上でイベント形式に変換し、トラップごとにわかりやすいメッセージテキストで表示するために、システム運用管理ソフトウェアのマネージャーへメッセージテキスト定義ファイルを登録します。

- **拡張 MIB 定義ファイルの登録**

  拡張 MIB は、各メーカーが独自のハードウェアに対して独自に作成した MIB で、この拡張 MIB をシステム運用管理ソフトウェアのマネージャーへ追加することで、対応したメッセージを表示することができます。

- **ServerView Operations Manager を操作メニューへ登録**

  システム運用管理ソフトウェアのマネージャーから、ServerView Operations Manager をそのまま起動できるようにメニューへ登録します。システム運用管理ソフトウェアが、ServerView Operations Manager の直接起動に対応している場合に限ります。

2.1.1 FUJITSU Software Systemwalker Centric Manager との連携

「FUJITSU Software Systemwalker Centric Manager」は、エンタープライズ環境における、システム、ネットワーク、アプリケーションなどの統合運用管理製品です。Microsoft Windows や各種 Linux や Unix、メインフレームなど、マルチプラットフォーム環境の統合運用監視が可能です。

共に富士通製品である「ServerView® Suite」と「FUJITSU Software Systemwalker」は、自社のソフト同士という強みを活かした高度な連携を実現することができます。

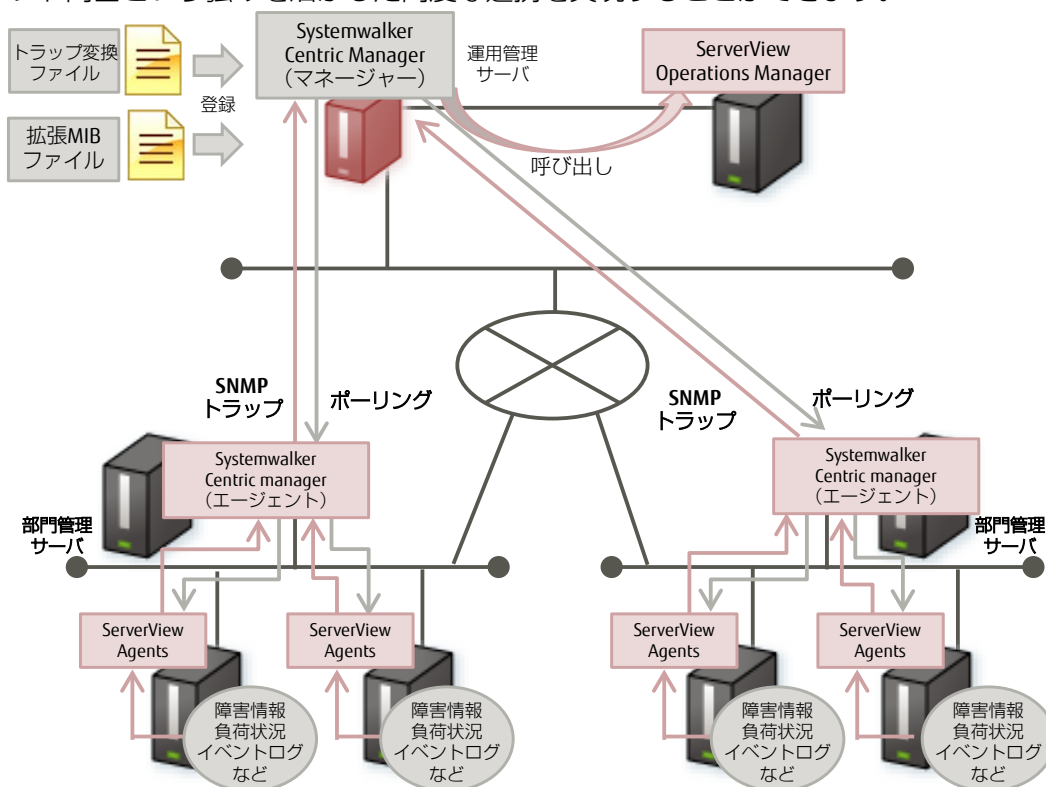



図 2-2 Systemwalker Centric Manager との連携イメージ

●連携によって可能になること

- 監視対象サーバで発生したハードウェア故障や、温度異常の詳細がメッセージで通知され、Systemwalker Centric Manager のコンソール上に表示されます。
- 各部門（単一セグメント）において ServerView Operations Manager が監視しているサーバのハード異常を、エンタープライズ環境において統合管理することができます。
- ServerView Operations Manager で受信したサーバからのメッセージを、条件で絞り込んで監視できます。
- Systemwalker Centric Manager の監視画面から、ServerView Operations Manager を直接起動し、異常の発生したサーバに対して、即座に ServerView Operations Manager 画面から対処できます。

2.1.2 FUJITSU Software Systemwalker Desktop Monitor との連携

FUJITSU Software Systemwalker Desktop Monitor は、Systemwalker Centric Manager の機能から、ネットワーク監視機能のみを切り出してリーズナブルに提供する、中・小規模システムのオフィスに最適なネットワーク監視ソフトウェアです。サーバ数台やクライアント数十台程度のシステムを、1 台の管理パソコンで簡単に監視できます。

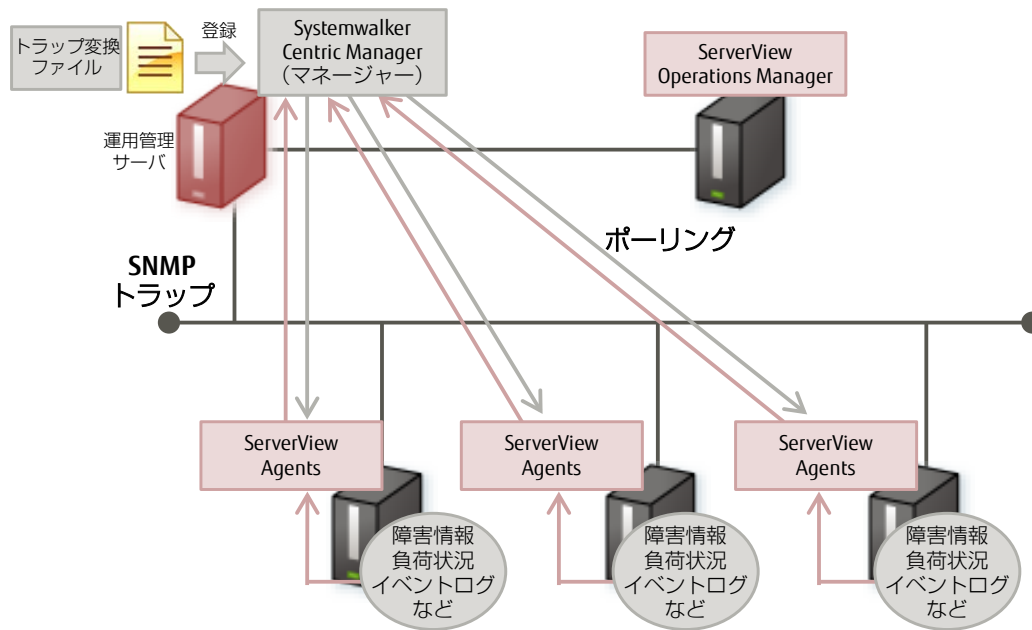



図 2-3 Systemwalker Desktop Monitor との連携イメージ

●連携によって可能になること

- 監視対象サーバで発生したハードウェア故障や、温度異常の詳細がメッセージで通知され、Systemwalker Desktop Monitor のマップ上に表示されます。

（注）

Systemwalker Desktop Monitor では、監視画面からの ServerView Operations Manager の起動、ServerView Agents からのトラップイベントの絞込み、サーバの MIB 値取得、MIB しきい値監視機能は使用できません。

2.1.3 Network Node Manager との連携

ServerView は、HP の OpenView Network Node Manager と連携することができます。それぞれの連携可能なバージョンの詳細については、お手持ちの「ServerView Operations Manager 取扱説明書」で、ご確認ください。

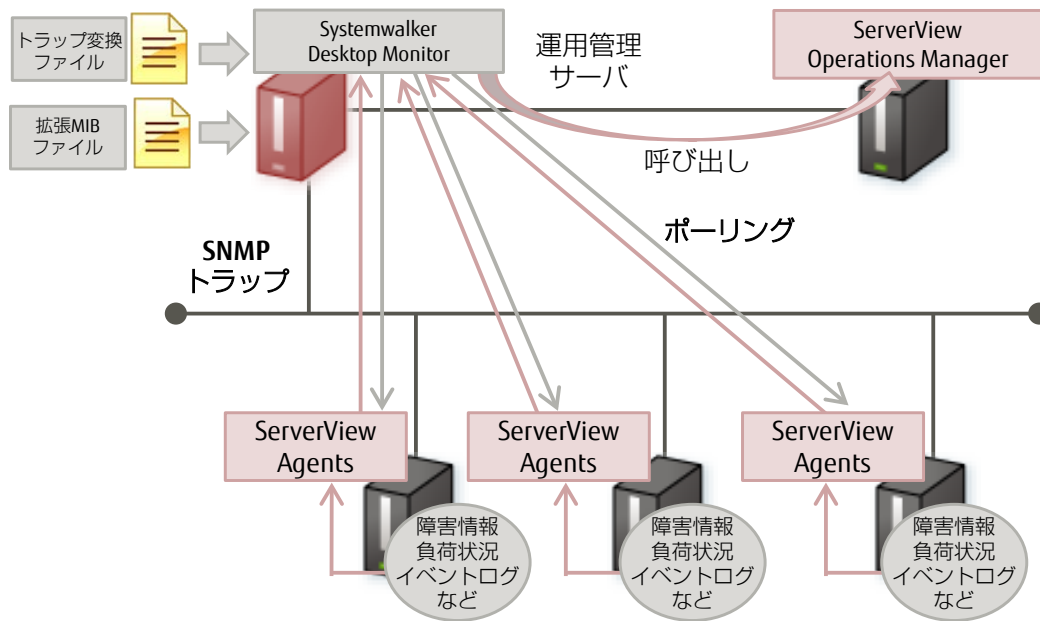



図 2-4 Network Node Manager との連携イメージ

●連携によって可能になること

- 監視対象サーバのハードウェアで発生した異常がメッセージで通知され、ServerView Operations Manager に表示されます。
- Network Node Manager の監視画面から、ServerView Operations Manager を直接起動し、監視イベントの詳細な調査や対処が可能です。

2.2 イベントログを経由する方法

ServerView Agents との SNMP トラップ連携に対応していないシステム運用管理ソフトウェアを利用する場合には、イベントログを経由した連携を行います。

「イベントログ」は、Windows® operating system に実装されている、各種動作の稼働状況を記録する一種のデータベースです（通常、「イベントビューア」という管理ツールを使用して、データを参照します）。

規格が定まっているイベントログを利用することで、ServerView と SNMP トラップ連携が不可能なシステム運用管理ソフトウェアと連携を行えるようになります。

「イベントログを経由する方法」とは、ServerView Agents の SNMP トラップ発生時にイベントログにトラップ情報を書き込み、システム運用管理ソフトウェアによる定期的なイベントログの確認により、SNMP トラップの発生を検知する方法です。

システム運用管理ソフトウェアのログ確認のタイミングで SNMP トラップを確認するため、トラップの発生から処理までにタイムラグが発生する場合があります。

例）

システム運用管理ソフトウェアのマネージャーが、イベントログの内容を確認する間隔が 10 分であった場合、イベントログにトラップが書き込まれてから、トラップの内容に応じた処理を実行するまでに、最大 10 分弱のタイムラグが生じる。

システム運用管理ソフトウェアによっては、監視対象サーバのイベントログを直接監視できない場合があります。本資料では、システム運用管理ソフトウェアが「監視対象サーバのイベントログを直接監視できる場合」と、「監視対象サーバのイベントログを直接監視できない場合」をご紹介します。使用するシステム運用管理ソフトウェアに合わせて、イベントログの書き込み場所やイベントログの取得手段を考慮し、連携システムを設計してください。

● ServerView Agents が作成するイベントログのルール

ServerView Agents は、以下のルールでイベントログを作成します。

ログの種類	：アプリケーション
ソース名	：**ServerView Agents**
イベント **ID**	：[**SNMP** トラップの **Specific** 番号] ＋ **10000**

ServerView Agents がイベントログに格納するログの詳細（意味、対処など）については、ServerView Operations Manager のマニュアルの「ServerView Event Manager」「PRIMERGY Server Events」をお読みの上、該当する SNMP トラップの［Specific 番号］を参照してください。

2.2.1 監視対象サーバのイベントログを直接監視できる場合

連携するシステム運用管理ソフトウェアが、監視対象サーバのイベントログを直接監視する機能がある場合の手順です。

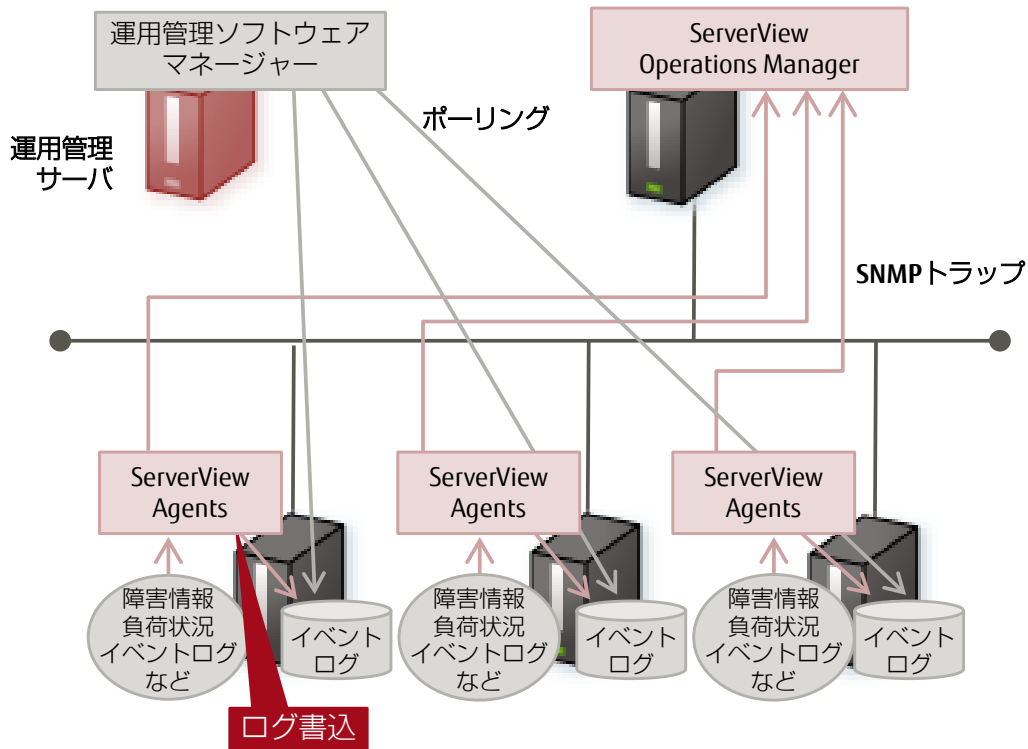



図 2-5 運用管理ソフトマネージャが監視対象サーバのイベントログを監視する場合のイメージ

① ServerView Agents は、監視対象サーバ上で何らかの問題が発生すると、イベントログに、トラップ情報を書き込みます。
② システム運用管理ソフトウェアのマネージャーの、リモート イベントログ管理機能を利用して、各サーバのイベントログに、トラップ情報が書き込まれたことを検知します。
③ システム運用管理ソフトウェアのマネージャーが、トラップ情報に応じた処理を行います。

2.2.2 監視対象サーバのイベントログを直接監視できない場合

連携させるシステム運用管理ソフトウェアが、監視対象サーバのイベントログを直接監視する機能が無い場合の手順です。

システム運用管理ソフトウェアのマネージャーが動作するサーバのイベントログへ、SNMP トラップ情報を書き込み、マネージャーは自分自身のイベントログを定期的に確認し、トラップの発生を検知します。運用管理サーバへイベントログを書き込む際に、ServerView Event Manager 機能（ServerView Operations Manager の機能の一つ）を利用するか、OS の機能を利用するかの違いにより、2 つのケースに分かれます。

≪ケース 1：ServerView Event Manager を利用≫

ServerView Event Manager 機能を利用し、ServerView Operations Manager が SNMP トラップを受信した場合に、ServerView Operations Manager が動作するサーバ（運用管理サーバ）のイベントログに情報を書き込みます。

ServerView Operations Manager とシステム運用管理ソフトウェアのマネージャーが、同一サーバ上にある場合に有効です。

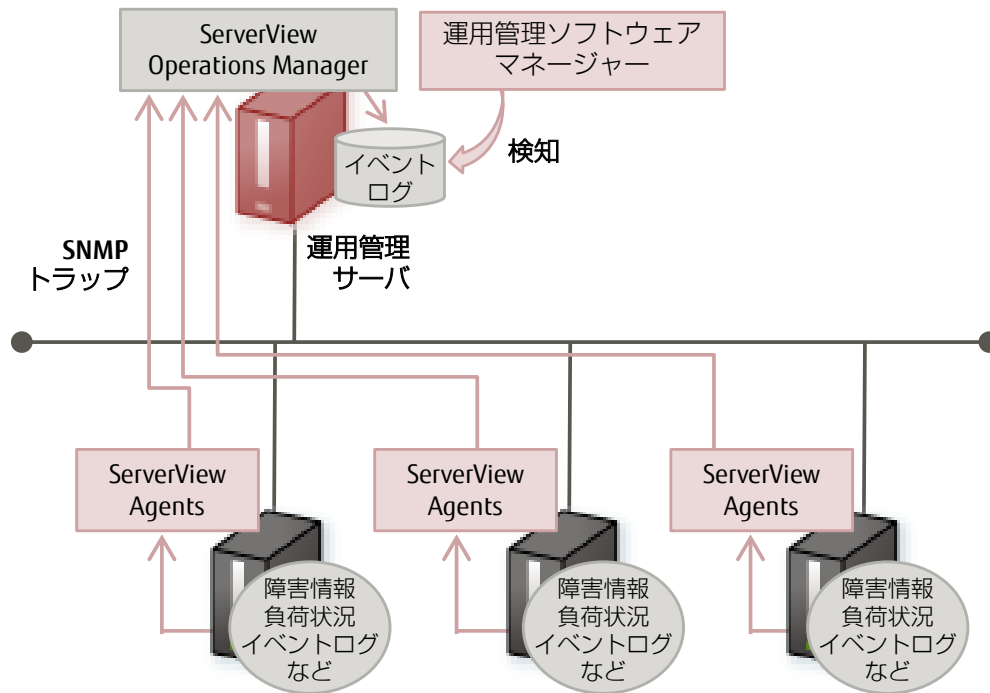



図 2-6 ServerView Event Manager を利用する場合のイメージ

① ServerView Agents は、管理するサーバ上で何らかの問題が発生すると、ServerView Operations Manager に対して、アラーム（SNMP トラップ）を送付します。

② ServerView Event Manager－「アラーム設定（共通設定)」で、ServerView Agents から送付されたアラームの内容を ServerView Operations Manager が動作するサーバ（運用管理サーバ）のイベントログに書き込むように設定します
→ここで、全ての「重要度」のチェックボックスを ON にすると、ServerView Agents から送付されたアラームを、運用管理サーバのイベントログに全て書き込めます。

③ システム運用管理ソフトウェアのマネージャーの、イベントログ管理機能を利用して、運用管理サーバのイベントログに、トラップ情報が書き込まれたことを検知します。

④ システム運用管理ソフトウェアのマネージャーが、イベントログに書き込まれた内容に応じた処理を行います。

なお、ServerView Operations Manager とシステム運用管理ソフトウェアのマネージャーが異なるサーバ上で動作している場合には、次の≪ケース 2：OS の機能を利用してイベントログを書き込む≫で紹介する方法で連携を実現することができます。

≪ケース 2：OS の機能を利用してイベントログを書き込み≫

OS の機能を利用して、運用管理サーバへイベントログを書き込みます。

図 2-7 OS の機能を利用してイベントログを書き込む場合のイメージ

① ServerView Agents は、監視対象サーバ上で何らかの問題が発生すると、監視対象サーバのイベントログにトラップ情報を書き込みます。
② 運用管理サーバのイベントログにトラップの発生を書き込みます。
→事前に、タスクスケジューラや OS に標準実装されたコマンドなどを利用して、特定の「イベント」発生をトリガーとして任意の処理を実行する設定をしておきます。
→この場合には、エージェントが SNMP トラップをマネージャーへ送信したのをトリガーとして、バッチの実行やタスクスケジューラの起動を設定しておき、運用管理サーバのイベントログへ書き込みや、ログの転送を行います。
③ システム運用管理ソフトウェアのマネージャーの、イベントログ管理機能を利用して、運用管理サーバのイベントログに、トラップ情報が書き込まれたことを検知します。
④ システム運用管理ソフトウェアのマネージャーが、運用管理サーバのイベントログに書き込まれた内容に応じた処理を行います。

上記の手順②は、エージェントが SNMP トラップをマネージャーへ送信したのをトリガーとして、バッチの実行やタスクスケジューラの起動を設定しておき、運用管理サーバのイベントログへの書き込みや、ログの転送を行います。

Windows® operating system のバージョンによって実現方法が異なります。

ここでは概要だけを紹介していますので、詳細な手順については各 OS のヘルプファイルなどを参照してください。

[Windows Server 2003]

Windows Server 2003 に標準搭載されている「eventtriggers」コマンドなどを組み合わせることで、システム運用管理ソフトウェアのマネージャーが動作しているサーバ上のイベントログへの書き込みを実現します。

[Windows Server 2008]、[Windows Server 2012]

Windows Server 2008 では、「タスクスケジューラ」が機能強化され、特定のイベントをトリガーとして、事前に設定されたタスクを自動的に実行させることができるようになりました。

Windows Server 2003 の場合と比べて、「eventtriggers」のような CUI コマンドを使用しなくて済む分、作業の手間が省けます。

また、イベントビューアの機能である「サブスクリプション（イベントの転送）」を利用して、リモートサーバのイベントログを収集することも可能です。

2.3 他社製運用管理ツールとの連携について

ここでは、他社製運用管理ソフトとの具体的な連携について、SNMP トラップを使った監視や、イベントログ監視を行い、障害情報の通知を行った際の検証結果を記載します。2.3.1 章では、日立の運用管理ソフト JP1 と PRIMERGY との連携について紹介します。2.3.2 章では、野村総合研究所の運用管理ソフト Senju Operation Conductor と PRIMERGY との連携について紹介します。2.3.3 章では、ServerView Operations Manager で障害情報の表示を確認したシステム運用管理ソフトウェアの一覧を紹介します。

2.3.1 JP1 との連携

- 監視対象サーバの障害情報を SNMP トラップで監視する場合

PRIMERGY に障害があった際の情報の通知について、下の図のような構成で確認しました。

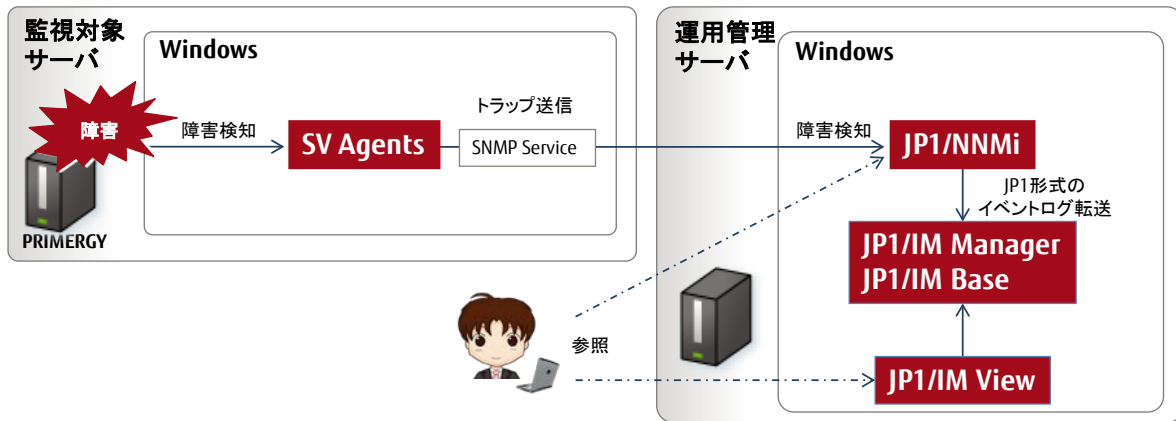



図 2-8 ServerView Agents と JP1 の連携

監視対象サーバの障害情報を SNMP トラップで送信し、JP1/Cm2/Network Node Manager i（JP1/NNMi）で受信します。また、JP1/NNMi で受信したメッセージは、JP1/ Integrated Management – Manager を通して JP1/ Integrated Management – View に表示されます。

JP1/NNMi の画面では、下の図のようにメッセージが表示されました。

図 2-9 JP1/Cm2/Network Node Manager i 上のメッセージ表示例

JP1/Integrated Management -View の画面では、下の図のようにメッセージが表示されました。

図 2-10 JP1/Integrated Management-View 上のメッセージ表示例

- 監視対象サーバの障害情報をイベントログで監視する場合

PRIMERGY に障害があった際の情報の通知について、下の図のような構成で確認しました。

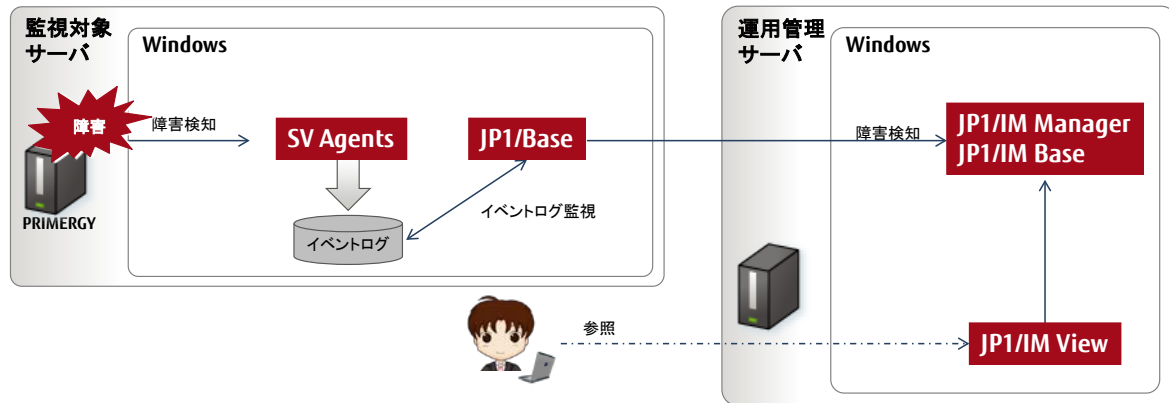



図 2-11 ServerView Agents と JP1 の連携

監視対象サーバの障害情報をイベンログに書き込みます。JP1/Base が検知したイベントログの情報を JP1/Integrated Management - Manager に通知します。また、JP1/ Integrated Management - View に受信したメッセージを表示します。

JP1/Integrated Management -View の画面では、下の図のようにメッセージが表示されました。

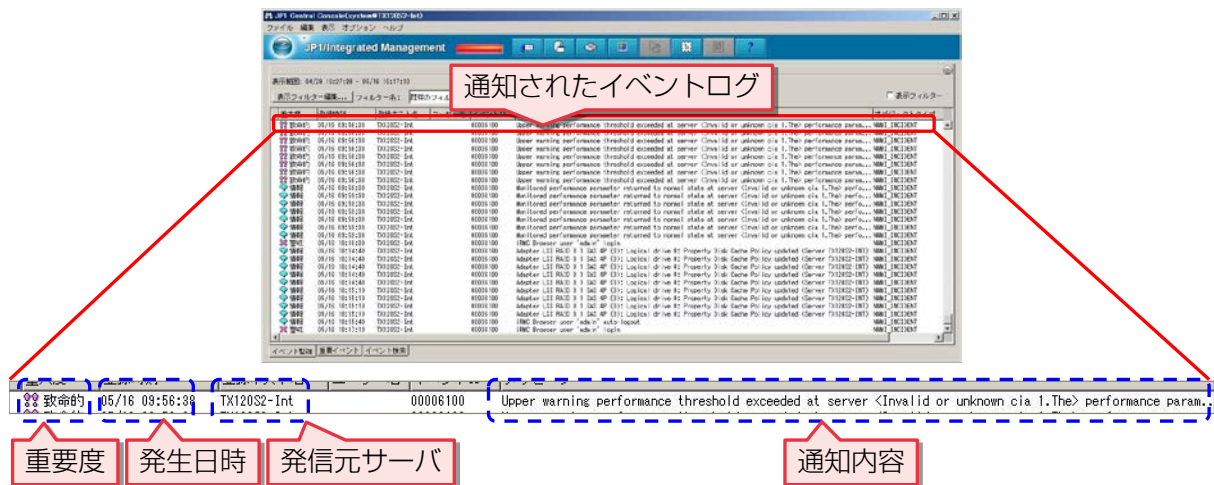



図 2-12 JP1/Integrated Management-View 上のメッセージ表示例

2.3.2 Senju との連携

- **監視対象サーバの障害情報を SNMP トラップで監視する場合**

PRIMERGY に障害があった際の情報の通知について、下の図のような構成で確認しました。

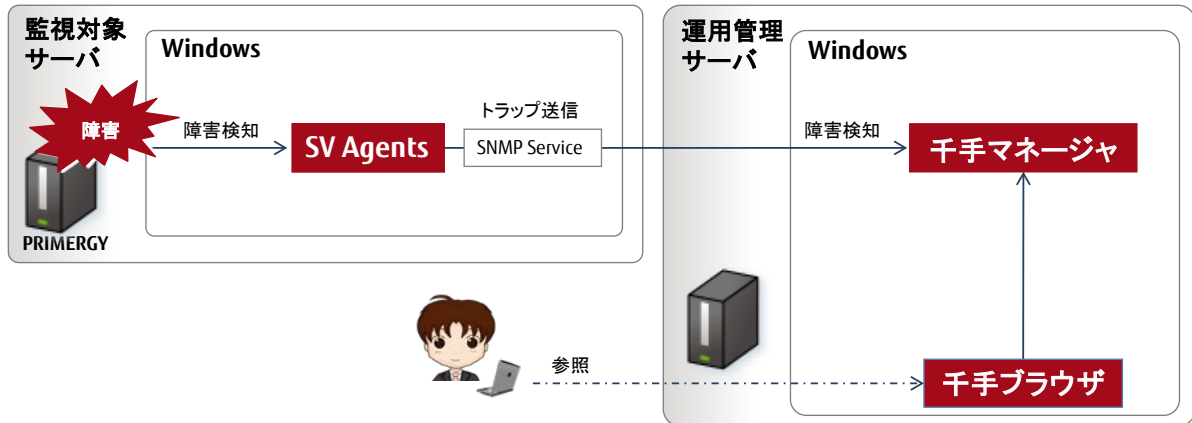



図 2-13 ServerView Agents と Senju の連携

監視対象サーバの障害情報を SNMP トラップで送信し、千手マネージャで受信します。また、千手マネージャで受信したメッセージは、千手ブラウザに表示されます。

千手ブラウザの画面では、下の図のようにメッセージが表示されました。

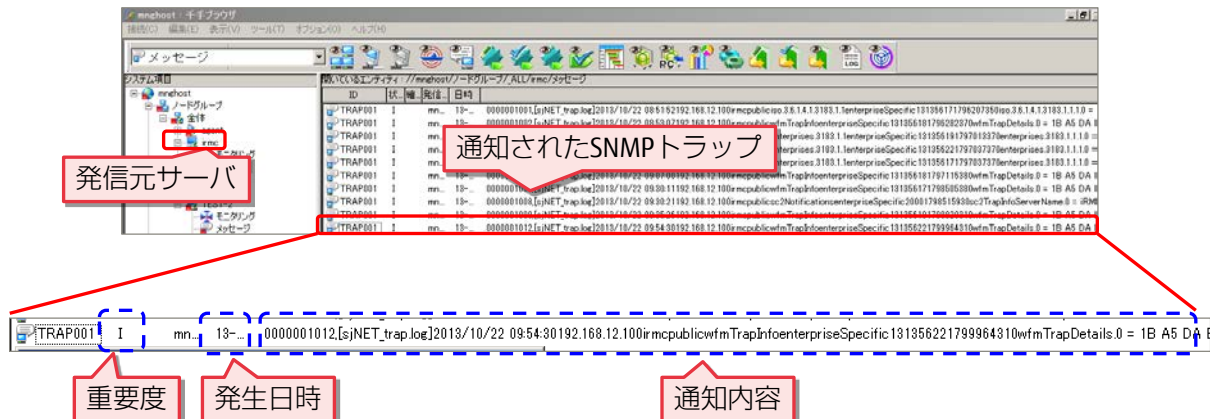



図 2-14 千手ブラウザ上のメッセージ表示例

SNMP トラップで監視する場合、重要度、通知内容が正しく表示されない場合がありますが、千手ブラウザのイベント機能を使うことで、重要度、通知内容が正しく表示されたことを確認しました。
その際、通知内容はSNMPトラップの通知内容ごとに用意したメッセージが挿入されて表示されます。

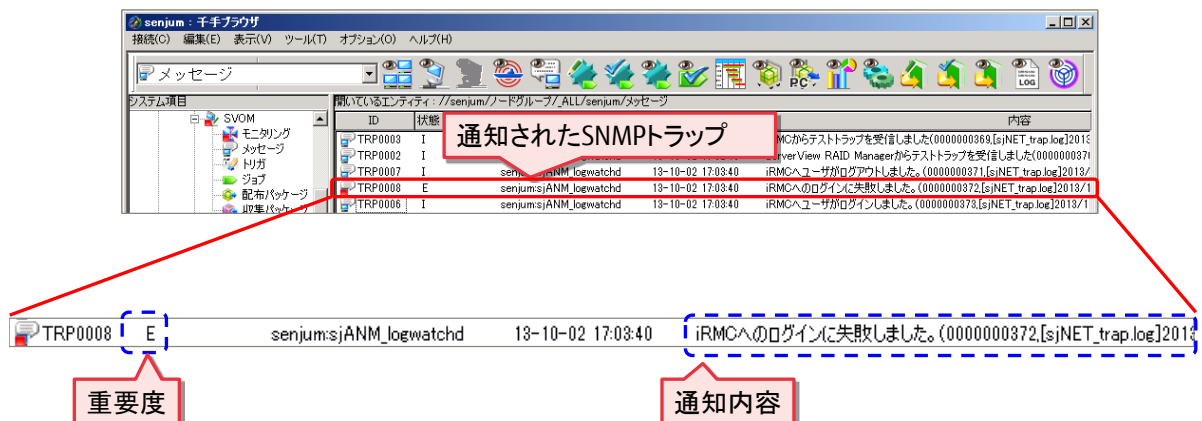



図 2-15 千手ブラウザ上のメッセージ表示例

・監視対象サーバの障害情報をイベントログで監視する場合

PRIMERGY に障害があった際の情報の通知について、下の図のような構成で確認しました。

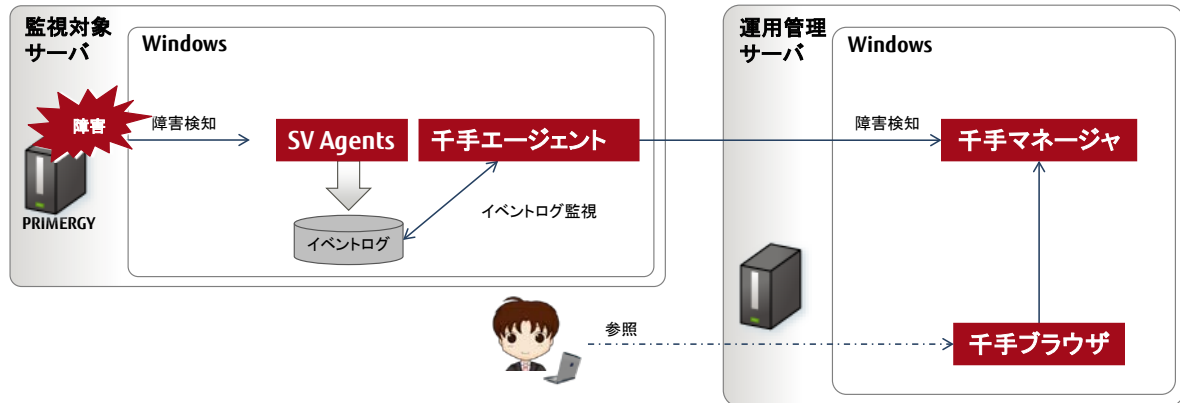



図 2-16 ServerView Agents と Senju の連携

監視対象サーバの障害情報をイベンログに書き込みます。千手エージェントが検知したイベントログの情報を千手マネージャに通知し、千手ブラウザに受信したメッセージを表示します。

千手ブラウザの画面では、下の図のようにメッセージが表示されました。

図 2-17 千手ブラウザ上のメッセージ表示例

2.3.3 システム運用管理ソフトウェア一覧

- 障害情報の表示を確認したシステム運用管理ソフトウェアの一覧

下の一覧表は、システム運用管理ソフトウェア上に PRIMERGY の障害情報が表示されるのを確認したものです。（注 1）

製品名
富士通 FUJITSU Software Systemwalker Centric Manager
富士通 FUJITSU Software Systemwalker Desktop Monitor
Microsoft System Center Operations Manager（注 2）
Microsoft System Center Configuration Manager（注 2）
HP OpenView Network Node Manager（注 2）
HP Operations Manager（注 2）
HP Systems Insight Manager（注 2）
IBM Tivoli Enterprise Console（注 2）
IBM Tivoli NetView（注 2）
VMware vCenter™ Server（注 2）
Nagios Enterprises Nagios（注 2）
The IcingaProject Icinga（注 2）
日立 JP1
野村総合研究所 Senju Operation Conductor

（注 1）

ここに記載がないシステム運用管理ソフトウェアも、SNMP トラップを受けられるものについては、基本的に同じ仕組みで連携できる可能性があります。

（注 2）

連携のための ServerView Integration Pack を提供

まとめ

本資料では、ServerView Operations Manager を他のシステム運用管理ソフトウェアに連携する仕組みとして、「SNMP トラップ連携による方法」と「イベントログを経由する方法」の２つを紹介しました。

システム運用管理ソフトウェアと ServerView Operations Manager の連携は、SNMP トラップ連携が利用できる場合には、より高度な連携と詳細な管理が実現可能です。PRIMERGY の運用管理には、標準添付の ServerView® Suite を有効に利用可能な、Systemwalker などの SNMP トラップ連携可能なシステム運用管理ソフトウェアの導入をおすすめします。

しかし実際の運用管理の場面では既にServerView Operations ManagerとのSNMPトラップ連携が不可能なシステム運用管理ソフトウェアを導入済みの場合や、他に導入する監視対象機器に対して推奨されるシステム運用管理ソフトウェアを導入する場合が多々あります。SNMP トラップ連携が行えない場合でも、ServerView Operations Manager の監視・管理機能を利用できるようにするために、システム運用管理ソフトウェア間で相互に利用可能であり、仕様が固定されている「イベントログ」を経由して連携させる方法をご紹介しました。システムの運用環境にあわせて最適な連携手段を検討してください。

なお、本資料をご覧頂き、実際に ServerView Operations Manager との連携を行う場合には、ServerView Operations Manager の各種マニュアル、および連携するシステム運用管理ソフトウェアのマニュアルも参照の上、十分な計画を立てて作業して頂けますようお願いします。

【添付資料】

SNMP バージョン情報

SNMP には、複数のバージョンが存在しますが、大まかに分類すると、v1～v3 までの 3 つのバージョンがあります。

- **SNMPv1 ［RFC 1155、1157］**

  Get / GetNext / Set / GetResponse / Trap の 5 つのコマンドが定義されています。

  最初に RFC（Request for Comments）で規定されたバージョンですが、既に基本的なコマンド定義が完成しているため、現在でも広く普及しています。

- **SNMPv2c ［RFC 1901、1905、1906］**

  コマンドのフォーマット（PDU：Protocol Data Unit）が拡張されており、GetBulk、INFORM request、Report が追加されましたが、仕組みが複雑となり、あまり普及していません。

  セキュリティレベル自体は、v1 と同等です。

- **SNMPv3 ［RFC 2576、3410～3418、3584、3826］**

  セキュリティ機能が強化され、PDU の暗号化が可能になりました。

  SNMP の欠点であるとされるセキュリティ機能が強化されており、このバージョンが普及して、旧バージョンが淘汰されることが期待されています。

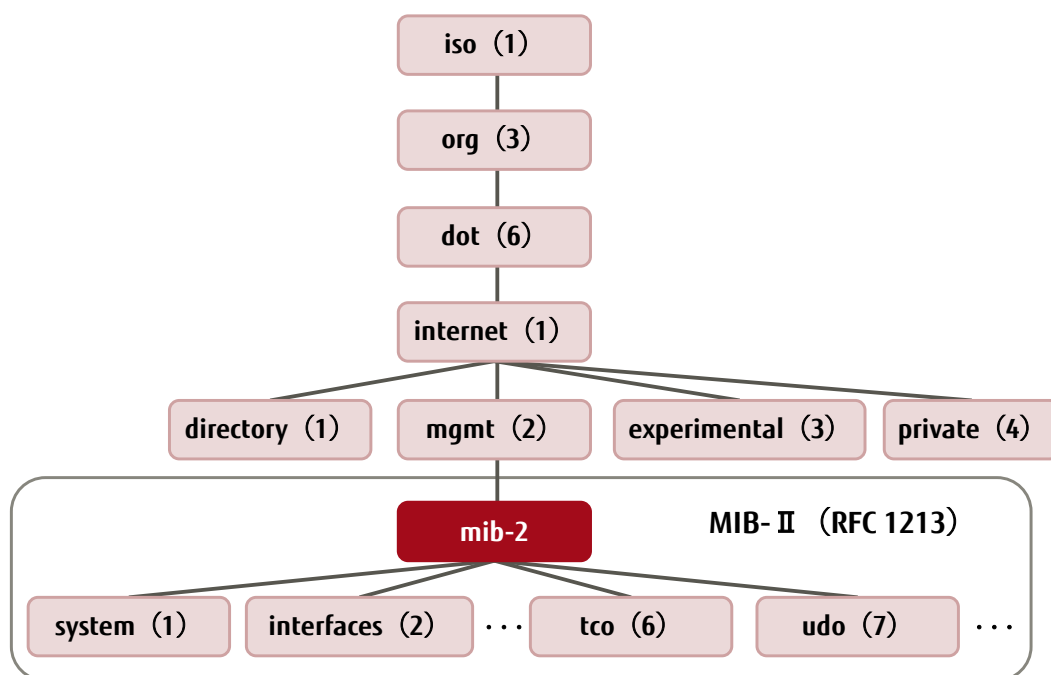
異なるシステム運用管理ソフトウェア同士の連携に際して、SNMP のバージョンの違いを意識する必要がある場合があります。

例えば、ServerView Operations Manager は、SNMPv1 / SNMPv2c に準拠したトラップのみをサポートしています。ServerView Agents for Windows は OS の標準の SNMP Service サービスを使用していますので、SNMPv1 で動作します。

MIB （Management Information Base：管理情報領域）

SNMP エージェントは、監視対象機器の情報を、MIB（Management Information Base）と呼ばれる「管理情報領域」を参照して、取得します。
MIB は、監視対象機器が自分自身の情報を保持するための、一種の「プロパティ」のようなものです。

MIB にも複数の版がありますが、通常、RFC で規定されている「標準 MIB」のことを指していると考えて、差し支えありません。
標準 MIB も、用途に応じて、MIB-Ⅰ、MIB-Ⅱ（RFC 1213）に分けられますが、現在は、MIB-Ⅱが主流になっています。
「標準 MIB」に対して、ベンダーなどが独自に拡張した MIB は、「プライベート MIB」や「拡張 MIB」などと呼ばれます。

MIB の実体は、下図のような階層構造であり、「MIB-Ⅱ」は、その一部を規定したものです。

MIB の階層構造と MIB-Ⅱの範囲

また、MIB に格納されている情報は、それぞれ「オブジェクト」と呼ばれる単位で管理されます。
「マネージャー」や「エージェント」が、特定のオブジェクトを指定する際には、各オブジェクトに割り当てられた「オブジェクト ID（OID）」という識別子を使用します。

商標登記について

- Microsoft Windows、Windows Server、及びその他の Microsoft 製品は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- VMware vCenter™は、VMware,Inc.の米国および各国での商標または登録商標です。
- JP1（JP1/Cm2/Network Node Manager i、JP1/Integrated Management、及びその他の JP1 製品）は、株式会社日立製作所の登録商標です。
- OpenView、Systems Insight Manager は、米国 Hewlett-Packard 社の商標または登録商標です。
- Tivoli（Tivoli Enterprise Console、及びその他の Tivoli 製品）は、世界の多くの国で登録された International Business Machines Corporation の商標です。
- Senju Operation Conductor（千手マネージャ、千手エージェント、千手ブラウザ、及びその他の千手製品）は、株式会社野村総合研究所の登録商標または商標です。
- Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標または商標です。
- Red Hat および Red Hat をベースとしたすべての商標とロゴは、米国およびその他の国における Red Hat, Inc. の登録商標または商標です。
- Nagios は、Nagios Enterprises 社の登録商標または商標です。
- Icinga は、米国およびその他の地域における The Icinga Project のオープンソースです。
- 記載されている会社名、製品名等の固有名詞は各社の商号、登録商標または商標です。
- その他、本資料に記載されている会社名、システム名、製品名等には必ずしも商標表示を付記しておりません。

免責事項

- 著作権・商標権・その他の知的財産権について

  本資料は、著作権・商標権・その他の知的財産権で保護されています。個人的に使用する範囲で本書をプリントアウトまたはダウンロードできます。ただし、これ以外の利用（資料の改変、ご自分のページへの再利用や他のサーバへのアップロード等）については、当社または権利者の許諾が必要となります。
- リンクについて

  本資料が掲載されているページは、連絡なしにリンクしていただいてかまいません。ただし、資料への直接のリンクや、フレームリンク、画像のみのリンク等、本サーバ上のコンテンツであることが不明確になるリンクは作成しないでください。
- 保証の制限

  本資料について、当社は、その正確性、商品性、ご利用目的への適合性等に関して保証するものではなく、そのご利用により生じた損害について、当社は法律上のいかなる責任も負いかねます。本書は、予告なく変更・廃止されることがあります。

FUJITSU Server PRIMERGY Web ページ： http://jp.fujitsu.com/platform/server/primergy/